

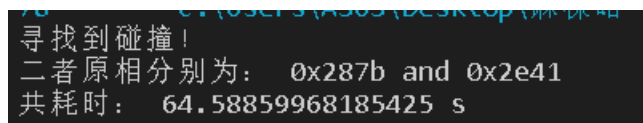
# Project: implement the naïve birthday attack of reduced SM3

## --寻找到碰撞的位数：前 7 位

代码说明：首先按照 sm3 算法把 sm3 的代码写出来，然后利用生日攻击构造碰撞：构造前 7 位碰撞，具体思路为输入大量随机数进入 sm3 函数，比较所有输出的前 6 位，发现相同的即碰撞完成。

运行指导：直接运行 py 文件

运行结果截图：



```
寻找到碰撞！  
二者原相分别为： 0x287b and 0x2e41  
共耗时： 64.58859968185425 s
```